derecom

ISSN: 1988-2629. Nº. 26. Nueva Época. Marzo 2019-Septiembre 2019

Cómo citar este texto:
Carolina López Medina. (2019). Protección de datos personales en la Administración de Justicia española: Protocolo de Comunicación de la Justicia 2018. *Derecom*, 26, 115-130. http://www.derecom.com/derecom/

PROTECCIÓN DE DATOS PERSONALES EN LA ADMINISTRACIÓN DE JUSTICIA ESPAÑOLA: PROTOCOLO DE COMUNICACIÓN DE LA JUSTICIA 2018

PERSONAL DATA PROTECTION IN THE SPANISH JUDICIARY: THE 2018 PROTOCOL ON THE JUDICIARY COMMUNICATIONS

© Carolina López Medina
Universidad de Jaén (España)
carolina_lmedina@hotmail.com

Resumen

Este artículo tiene por objeto abordar las particularidades del derecho fundamental a la protección de datos personales en el ámbito de la Administración de Justicia española, integrada por jueces y tribunales que, en el ejercicio de su potestad jurisdiccional y dentro de su competencia, tratan una gran cantidad de datos personales de los intervinientes en los procedimientos judiciales (partes, testigos). Así mismo, pone en conexión el citado derecho con el derecho a la libertad de información mediante el análisis de las principales medidas y recomendaciones que el Protocolo de Comunicación de la Justicia de 2018, elaborado por la Oficina de Comunicación del Consejo General del Poder Judicial, establece para que la información judicial, especialmente del orden penal, llegue a la sociedad de forma veraz, clara, eficaz y objetiva y con respeto a los derechos y libertades de los implicados.

Summary

In this contribution we try to examine the main particularities of the right to personal data protection in the Spanish Judiciary, made up of judges and courts that, in the practice of its powers, process a large amount of personal data of the individuals involved in judicial cases (parties, witnesess). Moreover, we aim to connect the above mentioned right with the fundamental right to information, though analysing the main measures and recommendations set by the 2018 Protocol on the Judiciary Communications, developed by the Communication Desk of General Council of the Judiciary, so that judicial information, particularly the criminal one, comes to society in a truthful, clear, effective and neutral manner and taking into account the rights and freedoms of the individuals involved in the cases.

Recibido: 19/12/2018 Revisado: 11/03/2019
Aceptado: 12/03/2019 Publicado: 15/03/2019

Palabras clave: Protección de datos. Información. Administración de Justicia. Protocolo de Comunicación de la Justicia. Ponderación de derechos.

Keywords: Data protection. Information. The Judiciary. Protocol on the Judiciary Communications. Balance of rights.

1.Introducción.

Vivimos en un mundo **global** e **interconectado** y, cada vez más, **digitalizado** en el que las Tecnologías de la Información y de la Comunicación (TIC) y la red de internet han cambiado nuestra vida en todos los aspectos y lo siguen haciendo con los continuos avances tecnológicos, como la inteligencia artificial o el internet de las cosas. Comprar por internet, utilizar el correo electrónico y las aplicaciones de mensajería instantánea como medio de comunicación, matricularse en la Universidad vía telemática, acceder a la jurisprudencia de forma on-line, suscribirse a aplicaciones o *blogs* de noticias son algunas de las tareas realizadas en las **sociedades tecnológicas** por las personas, empresas e instituciones, públicas y privadas.

Son múltiples los **beneficios** que dichas herramientas digitales ofrecen a la sociedad, la economía y, en particular, a la Administración de Justicia, inmersa desde hace años en un proceso de digitalización para tratar de mejorar la eficiencia y agilidad de la Justicia.[1] Sin embargo, **no todo es tan positivo.** Existe una ingente cantidad de datos personales de los intervinientes en los procedimientos judiciales (partes procesales, testigos, peritos), tanto los denominados normales o *regular data* (nombre, documento nacional de identidad, currículum vitae, imagen), como los sensibles o *categorías especiales de datos* (genéticos, biométricos, sanitarios, étnicos), que son objeto de tratamiento por Jueces y Tribunales, en el ejercicio de sus funciones y dentro de su competencia, y por la Oficina Judicial que sirve de soporte y apoyo a la actividad jurisdiccional, según la LO 18/2003, de 23 de diciembre, de modificación de la LOPJ. Los problemas surgen cuando dicho tratamiento se realiza de manera **ilícita**, al **margen de la normativa** y de la **ética**, toda vez que sus consecuencias son perjudiciales y de difícil reparación: la **vulneración del derecho fundamental a la protección de datos personales** y, por ende, el incumplimiento de la normativa sobre protección de datos.

El **régimen jurídico** a nivel **europeo** del derecho a la protección de datos, también denominado de *habeas data* o autodeterminación informativa, viene constituido por el Reglamento (UE) 2016/679, relativo a la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y a la Libre Circulación de estos Datos, más conocido como Reglamento General de Protección de Datos (**RGPD**, en adelante), aplicable directamente a todos los países europeos (art. 288 del Tratado de Funcionamiento de la UE) desde el 25 de mayo de 2018. También, la Directiva (UE) 2016/280, relativa a la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales por parte de las Autoridades Competentes para Fines de Prevención, Investigación, Detección o Enjuiciamiento de Infracciones Penales o de Ejecución de Sanciones Penales, y a la Libre Circulación de tales Datos (**Directiva** 2016/680, en adelante).

En el ordenamiento jurídico **español**, dicho Reglamento ha sido adaptado por la Ley Orgánica 3/2018, de Protección de Datos Personales y Garantías de los Derechos Digitales (**LOPDGDD**, en adelante) de noviembre, que deroga a la anterior Ley Orgánica 15/1999, de Protección de Datos, aunque el RGPD sigue teniendo aplicación directa. En cuanto a la referida Directiva, aún no ha sido traspuesta al Derecho nacional a pesar de haber transcurrido su plazo

de trasposición, sin perjuicio de que se plantee su **eficacia directa vertical** de conformidad con la jurisprudencia del Tribunal de Justicia de la UE.

La *protección de datos personales* es el **derecho fundamental** (art. 18. 4 CE) de toda persona física de controlar el uso y destino de su información personal. El Tribunal Constitucional español (TC, en adelante) ha precisado que es un derecho **autónomo** e independiente del derecho a la intimidad (art. 18.1 CE), *con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar (*…) (STC 292/2000, F. J. 5); y que

> *atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven para la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales (…) (STC 254/1993, F.J.7)*.[2]

Estos poderes, se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles por un tercero (STC 292/2000, F.J.7).

En el ordenamiento jurídico europeo sólo se protege la información personal de la persona física, tanto por el RGPD como por la Directiva 2016/689, a diferencia de otros países que tutelan también los datos de la jurídica o ideal,[3] como ocurre en Nicaragua, según lo dispuesto en la Ley nº 787, Ley de Protección de Datos Personales; o en la Iniciativa 4090-2009, Ley de Protección de Datos Personales de Guatemala. En cualquier caso, este derecho fundamental **no** es absoluto, sino que tiene limitaciones. Así, son frecuentes los conflictos con otros derechos y libertades fundamentales, como con el derecho de toda persona a la **libertad de información**, esto es, *a comunicar o recibir libremente información veraz por cualquier medio de difusión* (art. 20.1 d) CE).[4] En tales supuestos, nuestro TC viene manteniendo la prevalencia de la libertad de información *por su capacidad para formar una opinión pública libre, indisolublemente unida al pluralismo propio del Estado Democrático* (STC 21/2000). Prevalencia que no opera de forma automática *sino sólo en supuestos en los que no concurran otros factores en los que la ponderación lleve a primar la intimidad, el honor o la propia imagen, sobre las libertades de expresión, o en particular, de información* (STC 158/2003).[5] Por tanto, corresponderá al órgano judicial realizar una **ponderación** de los derechos en conflicto en el caso concreto.

En la actualidad, se han **incrementado** el número de **vulneraciones** del derecho a la protección de datos a nivel **nacional, europeo** e **internacional.** A modo de ejemplo, se traen a colación los casos de cesión de datos personales de millones de usuarios de la red social *Facebook* a una tercera empresa, sin previa información ni requerimiento del consentimiento de los titulares;[6] de filtración de los resultados y de la información de los participantes en los exámenes del Médico Interno Residente (MIR) y otras especialidades sanitarias;[7] la multa récord impuesta en enero de 2019 por la autoridad de control francesa al buscador de internet Google tras constatar el reiterado incumplimiento de la normativa europea sobre protección de datos;[8] la apertura de expediente por la Agencia Vasca de Protección de Datos (AVPD) al Ayuntamiento de Getxo (Vizcaya) tras la denuncia de la publicación en el tablón de anuncios

de la comisaría de una lista con las multas impuestas por cada agente en 2017 y su información personal, en enero de 2019.[9] Más recientemente, en marzo de 2019, la sala de lo contencioso-administrativo de la Audiencia Nacional ha confirmado una sanción de 40.000 euros impuesta por la Agencia Española de Protección de Datos (AEPD, en adelante) a la Asamblea Nacional Catalana por no proteger los datos de sus afiliados, publicados por terceros en las redes sociales en abril de 2014.[10]

Consecuencia del citado aumento del número de vulneraciones del derecho a la protección de datos, junto al incremento de las brechas de seguridad y de la cibercriminalidad, ha crecido el **interés y la preocupación social** por proteger la privacidad y la datos personales, siendo la protección de tales datos junto a la cibercriminalidad una de las principales preocupaciones de las empresas y las instituciones, públicas y privadas. ¿Las empresas, organizaciones e instituciones están cumpliendo la normativa sobre protección de datos? ¿Y la Administración de Justicia? ¿Cuál es la respuesta del ordenamiento jurídico para evitar la lesión del derecho a la protección de datos? ¿Cómo hacer posible la convivencia pacífica entre los derechos y libertades fundamentales? ¿Cómo se puede garantizar el derecho a la información a la vez que el derecho a la protección de datos en relación con la información judicial?

2.Particularidades de la protección de datos personales en la Administración de Justicia española.

Ante el **necesario tratamiento** de los datos de carácter personal de los intervinientes en los procedimientos judiciales (partes procesales, peritos, testigos) por parte de jueces y tribunales, así como por la Oficina Judicial que sirve de soporte y apoyo judicial, surge la obligación de asegurar a esos sujetos la adecuada protección **de su información personal**. Por ello y para garantizar la independencia judicial, la incorporación de datos a un procedimiento judicial tiene un **régimen jurídico particular o singular** que consiste en aplicar a la normativa europea general (RGPD y LOPDGDD) las especialidades previstas en la Ley Orgánica 6/1985, del Poder Judicial (LOPJ, en adelante) en la redacción dada por la Ley Orgánica 7/2015 (art. 236 bis a art. 236 decies), en todos los órdenes jurisdiccionales, excepto en el penal, donde es aplicable la Directiva 2016/680 con las especialidades previstas en la LOPJ. Como dicha Directiva no ha sido traspuesta al Derecho nacional, mantienen su vigencia los arts. 22 y ss. y sus disposiciones de desarrollo de la LOPD.[11]

El RGPD, en su considerando 20, expresa que, aunque se aplica a las actividades de tribunales y otras autoridades judiciales, pueden especificarse las operaciones de tratamiento y los procedimientos de tratamiento de datos realizados por ellos, en virtud del Derecho de la Unión o de los Estados miembros. El régimen jurídico particular de la protección de datos en la Administración de Justicia española es conforme a la legalidad vigente. El art. 236 bis LOPJ dispone que *el tratamiento de datos llevado a cabo con ocasión de la tramitación por los tribunales de los procesos de los que sean competentes, así como el realizado dentro de la gestión de la oficina judicial se someterá a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo, sin perjuicio de las especialidades establecidas en el presente capítulo*. Ahora procede señalar que las referencias contenidas en la LOPJ a la LOPD han de entenderse realizadas a la vigente normativa europea (RGPD y la LOPDGDD). Por su parte, el art. 2.4 LOPDGDD expresa literalmente lo mismo que el citado precepto pero con remisión expresa al RGPD y la LOPDGDD, indicando expresamente *in fine: sin perjuicio de las disposiciones de la Ley Orgánica 6/1985, del Poder Judicial que le sean aplicables*.

De forma sintética, del régimen jurídico particular de la protección de datos de carácter personal en la Administración de Justicia previsto en la LOPJ destacan las siguientes **particularidades**:

1ª Según el art. 236 ter LOPJ, los tribunales mantendrán los ficheros *necesarios para la tramitación de los procesos que en ellos se siguen, así como los que se precisen para su adecuada gestión*, con **respeto** a las garantías y derechos establecidos en la normativa sobre protección de datos personales. La particularidad es que se **diferencian** dos tipos de **ficheros** atendiendo a la naturaleza del tratamiento de los datos. Por un lado, los que contienen datos tratados con **fines jurisdiccionales,** en cuyo caso *el tratamiento se limitará a los datos en tanto se encuentran incorporados a los procesos de que conozcan y su finalidad se relacione directamente con el ejercicio de la potestad jurisdiccional*, es decir, todas las resoluciones judiciales ya sean dictadas por el Poder Judicial o por el Letrado de la Administración de Justicia. Por otro, los **no jurisdiccionales,** que son aquellos que constan *en procedimientos gubernativos tramitados por Juzgados y Tribunales* (art. 87.1 Reglamento CGPJ 1/2005, sobre Aspectos Accesorios de las Actuaciones Judiciales).

2ª **No será necesario el consentimiento del interesado** para que los tribunales traten los datos en el ejercicio de la potestad jurisdiccional, ya sean facilitados por las partes o recabados a instancia del Tribunal,

> *sin perjuicio de lo dispuesto en las normas procesales para la validez de la prueba. Cuando se trate de datos tratados con fines no jurisdiccionales se estará a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre*. (art. 236 quáter LOPJ)

Nuevamente hemos de entender que la remisión a la LOPD se hace a la actual normativa general de protección de datos (RGPD y LOPDGDD).

Al igual que en el régimen general, se exige una base de legitimación de las previstas en el art. 6 RGPD para que el tratamiento sea considerado lícito, pero en este ámbito **no se aplica el consentimiento como base de legitimación** del tratamiento en ficheros jurisdiccionales, sino que serán de aplicación otras de las bases de legitimación, normalmente, el cumplimiento de una misión realizada en interés público y en el ejercicio de **poderes públicos** conferidos al responsable del tratamiento; o el cumplimiento de una **obligación legal** aplicable al responsable. En definitiva, el ejercicio de la potestad jurisdiccional es base legítima para el tratamiento de datos en ficheros jurisdiccionales, sin perjuicio de lo que dispongan las reglas para la validez de la prueba, teniendo que acudir a las reglas de la Ley de Enjuiciamiento Civil (LEC, en adelante) o Ley de Enjuiciamiento Criminal (LECR, en adelante), según se trate.

3ª

> *(…) será **responsable de los ficheros jurisdiccionales el órgano jurisdiccional u oficina judicial** ante el que se tramiten los procesos cuyos datos se incorporen al fichero, y dentro de él decidirá quien tenga la competencia atribuida por la normativa vigente de acuerdo a la solicitud que se reciba del ciudadano. Igualmente, será responsable respecto de los ficheros no*

> *jurisdiccionales la Oficina judicial correspondiente al órgano judicial con el que se relacionen los datos que a los mismos se incorporen* (art. 236 sexies 1 LOPJ).

Mientras que en el régimen general, el responsable es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; y el encargado es la persona que trata los datos personales por cuenta del responsable (art. 4 RGPD). Además, las Administraciones Públicas competentes en materia de dotación de medios materiales a la Justicia, cada una en su ámbito, son **corresponsables** del tratamiento de ficheros jurisdiccionales, toda vez que diseñan, implementan y aplican el Sistema de Gestión Procesal y el Expediente Judicial Electrónico,[12] debiendo dotarlos de los mecanismos de seguridad, prevención y tutela del derecho a protección de los datos personales.

4ª **El Consejo General del Poder Judicial** (CGPJ en adelante), órgano de gobierno de jueces y tribunales, es la **autoridad de control** del cumplimiento de la normativa sobre protección de datos en la Administración de Justicia española en relación con los **ficheros jurisdiccionales** (236 nonies 1 LOPJ). Mientras que los tratamientos con fines no jurisdiccionales son competencia de la AEPD, a la que el CGPJ prestará la colaboración que al efecto precise, según el art. 236 nonies 2 LOPJ, pudiendo adoptar las medidas reglamentarias que estime para garantizar el cumplimiento de las medidas de seguridad conforme a la normativa sobre protección de datos respecto a los tratamientos de datos con fines no jurisdiccionales.

El RGPD en su considerando 20 expresa que, a fin de preservar la independencia judicial en el desempeño de sus funciones, incluida la toma de decisiones, la competencia de las autoridades de control no ha de abarcar el tratamiento de los datos cuando los Tribunales actúen en ejercicio de la función jurisdiccional, sino que el control ha de encomendarse a *organismos específicos establecidos dentro del sistema judicial del Estado miembro*, que deben **garantizar** el cumplimiento de las normas de protección de datos, **concienciar** más a los miembros del Poder Judicial sobre sus obligaciones en esta materia y atender las **reclamaciones** para con el tratamiento de datos. El art. 55.3 RGPD dispone que las autoridades de control no serán competentes para controlar las operaciones de tratamiento efectuadas por los tribunales en el ejercicio de la función judicial.

Según la LOPJ y la LOPD, el CGPJ ejerce las competencias atribuidas a la AEPD y según la LOPDGDD, ambas colaborarán *en aras del adecuado ejercicio de las respectivas competencias que la LOPJ les atribuye en materia de protección* (art. 44.3 LOPDGDD), por lo que indudablemente el citado órgano de gobierno de jueces y tribunales es la autoridad de control en el cumplimiento de la normativa sobre protección de datos en relación con los ficheros jurisdiccionales. En consecuencia, no se considera necesario crear un nuevo organismo específico de control. No obstante, en caso de que así se considere, se podrían reforzar su independencia en el ejercicio de su función de autoridad de control, de conformidad con el RGPD.

A pesar de dicho régimen de regulación de la protección de datos en la Administración de Justicia, también en este ámbito puede lesionarse el derecho a la protección de datos si no se toman las medidas adecuadas de seguridad, prevención y tutela. Al respecto, se trae a colación el caso de **filtración de datos personales de la víctima en la sentencia de la Audiencia Provincial de Navarra nº 38/2018,** comúnmente conocida como la sentencia de *La Manada*,

que fue comunicada por la Oficina Judicial con el Código Seguro de Verificación (CSV), por lo que terceros tuvieron acceso al contenido íntegro de la misma sin la previa obligación de disociación de datos que ordena la LOPJ, incumpliéndose la normativa sobre protección de datos y vulnerándose tal derecho. Ante este hecho, el Gabinete Técnico del CGPJ publicó un **Informe-Propuesta**[13] aclarando que la citada filtración fue resultado de un conjunto de factores de diversa índole, como la rapidez y la presión mediática en conocer la resolución, que *incidieron en el cumplimiento de la obligación de disociación de datos de carácter personal*, establecida en los arts. **235 bis y 266 LOPJ** y en general, en el cumplimiento de las disposiciones relativas al tratamiento de los datos dentro del ámbito de aplicación del RGPD, de los arts. 236 bis y 236 decies LOPJ y en la LOPD; calificando de ***sistémico*** el origen causal de la divulgación. A la mencionada obligación de disociación de datos personales nos referiremos en el apartado *3.3. Protección de datos personales en las resoluciones judiciales*.

Del citado Informe-Propuesta destacan dos consideraciones **positivas.** Por un lado, la propuesta a la Comisión Permanente del traslado del acuerdo a las instancias judiciales y administrativas competentes para que adopten las medidas necesarias *para procurar que quienes tienen encomendadas las distintas responsabilidades en materia de publicidad, comunicación y difusión de las resoluciones judiciales puedan ejercerlas en un contexto de seguridad técnica y de respeto a la normativa de protección de datos*. Por otro, la propuesta a los órganos técnicos del Consejo de que lleven a cabo las actuaciones precisas para elaborar una **guía de recomendaciones** en la aplicación de la normativa sobre protección de datos personales dirigida a los integrantes de la carrera judicial, en la que actualmente se está trabajando. Es decir, no solo reconoce dicho error sistémico, sino que va más allá y manifiesta una voluntad de publicidad y responsabilidad proactiva para con la normativa sobre protección de datos y el principio de transparencia.

Los acontecimientos de filtraciones de datos en la Administración de Justicia española, como el expuesto sobre la Sentencia de *La Manada*, la brecha de seguridad del sistema LexNet, de notificación de resoluciones judiciales en 2017, por la que se dejó al descubierto documentos judiciales alojados en él con datos personales;[14] o como la noticia de recogida por la Justicia de documentos judiciales con datos personales en un contenedor de los Juzgados de Valencia,[15] inciden **directamente** en la percepción de la ciudadanía de la justicia como ***mejorable*** y ponen en cuestión el tratamiento de los datos por parte de la Administración de Justicia.

Por tanto, las últimas reformas legales conllevan la conveniencia de que los órganos competentes elaboren una regulación **sistemática, completa y desarrollada de la protección de datos personales en la Administración de Justicia española,** pues el actual régimen contenido en tan solo nueve artículos con remisiones a la antigua LOPD 1999 y a otras normas procesales deviene insuficiente. En el mismo sentido que el Informe Complementario al emitido sobre el Anteproyecto de la LOPD, aprobado por el Pleno del CGPJ de 26 de julio de 2017. No obstante, hemos de ser **positivos**. Se va por buen camino y se ha avanzado considerablemente en cuanto a la protección de datos en este ámbito; pero también realistas: siempre se puede y se debe mejorar.

Es importante **aprender de los errores pasados para proyectar que no se vuelvan a repetir en el futuro.** Seguir trabajando en la consecución del **objetivo común**, un mayor nivel de protección de datos; seguir **formando y actualizando** periódicamente sobre la protección de datos al personal integrante y al servicio la Administración de Justicia; y fomentando la **colaboración** y coordinación de todas las instituciones (Poder Judicial, la Oficina Judicial, las

Administraciones Públicas competentes en materia de dotación de medios materiales, CGPJ) en la protección de los datos de los intervinientes en los procesos judiciales favorecerá la tutela y la responsabilidad proactiva en el cumplimiento de este derecho fundamental en el ámbito judicial.

3. Protocolo de Comunicación de la Justicia de 2018.

El **Protocolo de Comunicación de la Justicia de 2018** es un documento elaborado por la Oficina de Comunicación del CGPJ, que pone al día el anterior de 2015[16] de reformas legales y de las nuevas formas de comunicación que someten a un mayor riesgo los datos personales. De ahí, que este incluya un nuevo apartado, el sexto, dedicado a la protección de datos de carácter personal.

La **actividad de los órganos judiciales** genera información judicial de gran **interés social y periodístico**, especialmente la derivada del ámbito penal. Los ciudadanos son titulares del **derecho fundamental** a la protección de **sus datos de carácter personal** (art. 18.4 CE), pero también del derecho a la libertad de **información veraz por cualquier medio de comunicación,** en relación con el principio constitucional de publicidad de actuaciones (art. 120.1 CE), por lo que en el ejercicio de este último derecho cumplen un papel esencial los medios de comunicación. En el ámbito de la Administración de Justicia española, las **Oficinas de Comunicación** son el **cauce institucional de la información judicial** sobre asuntos de interés y que consideren que deben *ser conocidos por la opinión pública por su trascendencia y relevancia social o jurídica*. Son el instrumento institucional de conexión del Poder Judicial con los medios de comunicación y con la sociedad directamente a través de las redes sociales. La Oficina de Comunicación del CGPJ es la que marca los criterios en política de comunicación a las demás, creadas en el Tribunal Supremo, en la Audiencia Nacional y en los Tribunales Superiores de Justica de las Comunidades Autónomas.

Volviendo al Protocolo de Comunicación de la Justicia, refleja tres consideraciones cargadas de razón. Que la publicidad de las actuaciones judiciales se verá reforzada con una **política de comunicación institucional** *que traslade de forma cohesionada, reconocible y veraz la realidad del Poder Judicial español a través de canales de comunicación profesionales, estables y adecuados para trasmitir a los ciudadanos, últimos destinatarios de la actividad jurisdiccional, las decisiones y resoluciones de mayor trascendencia y relevancia social*. Que debe existir una relación de **confianza** entre miembros de las Oficinas de Comunicación, jueces y magistrados y sus órganos de gobierno. Por último, que *una comunicación efectiva exige la **colaboración** de todos*, lo que permitirá actuar con previsión ante *asuntos o resoluciones de relevancia social e interés público, evitando la apariencia de ineficacia, las filtraciones interesadas y las interpretaciones erróneas*.

A continuación, se exponen en los subapartados siguientes las medidas y recomendaciones que el Protocolo de Comunicación de la Justicia 2018 contiene para garantizar el derecho a la información derivada de los tribunales de forma *eficaz, clara, veraz, objetiva y responsable* con absoluto respeto a los derechos de los implicados en los procesos judiciales, especialmente del orden penal, tanto en la fase de instrucción o investigación penal, como en la de juicio oral y en la de publicación de las resoluciones judiciales.

3.1.Recomendaciones para la protección de datos en la fase de instrucción penal

En la fase de instrucción del proceso penal, **hasta que se declare la apertura del juicio oral las diligencias del sumario serán secretas,** según el art. 301 de la LECRim. Ahora bien, como ha

declarado el TC, tal precepto requiere *una interpretación estricta, no siendo su mera alegación fundamento bastante para limitar más derechos -ni en mayor medida de lo necesario- que los afectados por la norma entronizadora del secreto* (STC 13/1985, de 31 de enero).

Conforme a lo anterior, el Protocolo permite a las Oficinas de Comunicación facilitar la **información y las resoluciones procesales de asuntos relevantes, previa autorización del Juez instructor, siempre que no se trate de las diligencias de sumario y no perjudique la finalidad de secreto sumarial** (alcanzar una segura represión del delito). Nos referimos a la información sobre los autos de admisión o inadmisión a trámite o los que ordenan la prisión provisional u otras medidas cautelares. También, pueden facilitar y actualizar información referida a aspectos como el número e identidad de los investigados y/o defendidos que han declarado judicialmente y los motivos de su imputación y/o detención, con una breve descripción de los hechos o indicios del delito; la situación procesal acordada tras la declaración; las pruebas periciales realizadas o las diligencias de investigación practicadas.

Según el Protocolo, la experiencia ha demostrado que ello no perjudica el secreto de sumario ni el buen fin de la investigación, sino que contribuye a **ensalzar** la labor judicial y facilitar la comprensión de jueces y tribunales por la ciudadanía, algo deseable porque la única relación que la mayoría de los ciudadanos tienen con la Justicia es a través de la información judicial difundida a través de los medios de comunicación. Así pues, que la primera información que se conozca socialmente sobre un suceso sea institucional, oficial, con todas las garantías legales, evita filtraciones e interpretaciones erróneas o indeseadas.

El derecho a la información se garantiza en el citado Protocolo hasta el punto de que en los casos de gran repercusión mediática la información se pone a disposición de la Oficina de Comunicación de forma simultánea a su notificación a las partes. Ello puede tener el inconveniente de generar presión mediática y social a la Justicia, afectando en este caso al principio de independencia judicial (arts. 117.1 CE en relación con el art. 14.1 LOPJ). De todas maneras, como el derecho la información debe **convivir** con otros derechos fundamentales y principios constitucionales, ha de ejercerse de conformidad con la ley, con el máximo respeto al buen fin de la investigación, al derecho fundamental la tutela judicial efectiva y a los derechos fundamentales y a las libertades de los implicados (presunción de inocencia, protección de su honor, de su intimidad y de sus datos personales).

En cuanto a los **medios de comunicación audiovisuales,** en fase de **instrucción,** según el Protocolo, *deben poder tener acceso a la imagen que se produce en el exterior de los juzgados, ya sea de investigados o testigos, con los límites que establece la ley*; y se les *debe facilitar el trabajo en los exteriores*, teniendo prioridad la garantía del funcionamiento de las Administración de Justicia y sin perturbar la normal actividad judicial. Como recomendación propone que se mantenga abierto un espacio o facilite un lugar en el que los medios de comunicación puedan trabajar fuera del horario de audiencia, siempre que sea posible.

Todas las medidas son adecuadas en relación con la protección de datos personales. No son obligatorias, pero es conveniente que tanto las Oficinas de Comunicación como los medios de comunicación sigan sus recomendaciones. Como última consideración, cabe plantear la posibilidad de establecer unas sanciones para aquellos casos en los que dichos medios difundan información sobre sucesos o noticias judiciales en fase de instrucción de forma indebida, excesiva, incumpliendo el criterio judicial, produciendo filtraciones indeseadas, difundiendo información personal de tal modo que se cause un perjuicio real y

efectivo al secreto de sumario, la frustración directa de la represión o la vulneración del delito o al honor, la intimidad y la protección de los datos personales de los implicados.

3.2.Recomendaciones para la protección de datos en la fase de juicio oral

Según la LECrim, *los debates del juicio oral serán públicos, bajo pena de nulidad* (arts. 301 y 680 LECRim). Así, desde que se declara judicialmente el fin de la fase de instrucción, **el proceso judicial se convierte en público y, en principio, no hay restricciones de acceso a la vista y a la información, salvo en casos excepcionales señalados por la ley,** como en casos en que estén implicados menores o de violencia de género. Sin embargo, el art. 680 de la LECrim dispone que mediante **auto motivado** *podrá, no obstante, el presidente mandar que las sesiones se celebren a* ***puerta cerrada*** *cuando así lo exijan razones de moralidad o de orden público, o el respeto debido a la persona ofendida por el delito o su familia*. En igual sentido, según el art. 232 de la LOPJ, *excepcionalmente por razones de orden público y de protección de derechos y libertades, los jueces y tribunales, mediante resolución motivada, podrán limitar el ámbito de la publicidad y acordar el carácter secreto de todas o parte de las actuaciones*.

El principio constitucional de publicidad de las vistas orales ha sido amparado por el TC, que ha reconocido el derecho a los periodistas de acceder a las mismas, pues *forma parte del contenido de su derecho a comunicar información la obtención de la noticia en la vista pública en la que ésta se produce*. El Reglamento 1/2005, sobre los Aspectos Accesorios de las Actuaciones Judiciales, dispone, en su art. 6, que

> *se permitirá, con carácter general, el acceso de los medios de comunicación acreditados a los actos procesales celebrados en audiencia pública, excepto en los supuestos en que pueden verse afectados valores y derechos constitucionales, en los que el Juez o Presidente podrá denegar dicho acceso mediante resolución motivada.*

En virtud de lo anterior, el Protocolo dispone que las Oficinas de Comunicación *deberán* ***informarse*** *con la suficiente antelación de la existencia o no de resoluciones* judiciales al amparo del citado artículo 6 en todas las *vistas orales de relevancia pública y se ocuparán de dar traslado de las mismas a los periodistas*; y en segundo lugar, si se acuerda *celebrar una vista a puerta cerrada sin haber dictado resolución motivada al respecto, la oficina de comunicación pedirá al juez o presidente del tribunal que la dicte y se la trasladará a los periodistas.*

En cuanto a los **medios de comunicación audiovisuales** en fase de juicio oral, el Protocolo advierte que no se ha regulado el acceso de este tipo de medios a las salas de vistas y reproduce la doctrina constitucional que declara que la regla general es el libre acceso de aquéllos a las vistas, salvo que en los casos previstos en la ley se limite o restrinja el derecho a la información de estos medios. Las Oficinas de Comunicación solicitarán resolución motivada de ese acuerdo y la trasladarán a los periodistas.

Por otra parte, establece criterios para la grabación de imágenes de las partes en la vista oral, con **recomendaciones en la grabación de imágenes** para conciliar el derecho a la información con los derechos al honor, la intimidad y a la propia imagen de los intervinientes, tales como colocar las cámaras de manera que no molesten y siguiendo las indicaciones del tribunal, apagarlas durante los recesos y cuando el juicio haya quedado visto para sentencia; o

evitar grabar imágenes que permitan identificar a las víctimas salvo que hayan prestado expresamente su consentimiento.

También, establece la prioridad del uso del medio de grabación propio de calidad y la distribución de imágenes entre los medios que lo soliciten, poniendo la Oficina de Comunicación *los medios técnicos necesarios para que esa señal sea recogida por los medios de comunicación*; y que la imagen que faciliten sea siempre institucional, con imágenes a medio plano de la persona interviniente y evitando planos que contribuyan al sensacionalismo o a ofrecer una visión sesgada de la vista oral. Al respecto, Carlos Berbell exponía la importancia de la realización por parte de los dichos medios de comunicación, advirtiendo que no es lo mismo la grabación por una televisión comercial o privada que la realizada por uno institucional y que, en cualquier caso, hay que intentar la grabación de planos de la vista de forma que no condicionen la visión o la opinión del espectador.[17]

En cuanto al sistema de grabación, recomienda que si la sala de vistas es pequeña, no se puedan colocar varias cámaras de televisión y no existe imagen institucional, se organice un *sistema de pool* (un medio graba y distribuye). Si aun así no es posible, *se organizará un mudo* (grabación de imágenes al inicio del juicio). Igualmente, sugiere que las Oficinas de Comunicación ofrezcan un trato **igualitario** a los medios, lo cual da virtualidad al principio de igualdad (art. 14 CE), contemplando que la información se proporcione a todos a la vez *salvo que se trate de informaciones, entrevistas o reportajes solicitados por un medio concreto*. Incluso posibilita que habiliten canales de comunicación o **grupos** de difusión en aplicaciones instantáneas, como *WhatsApp*, medios muy utilizados por los jefes de prensa y los periodistas, quienes los valoran positivamente al permitirles estar informados de la fuente oficial, de forma inmediata y en condiciones de igualdad.

En cuanto a los **funcionarios** que intervienen en la vista (jueces y magistrados, fiscales, letrados de la Administración de Justicia, médicos forenses y peritos funcionarios), se remite a la LO 1/1982, sobre Protección Civil del Derecho al Honor, la Intimidad y a la propia Imagen, según la cual el derecho a la propia imagen **no impedirá**

> *su captación, reproducción o publicación por cualquier medio, cuando se trate de personas que ejerzan un cargo público o una profesión de notoriedad o proyección pública y la imagen se capte durante un acto público o en lugares abiertos al público*.

Por último, interesa señalar que **España** es uno de los países con **mayor transparencia informativa en la retransmisión de juicios**.[18] Muestra de ello es la retransmisión completa y en directo del denominado *Juicio del Procés*, que se está enjuiciando en el Tribunal Supremo, a la que se puede acceder desde cualquier parte del mundo en la web del CGPJ. Además, en los medios de comunicación e informativos, incluso en *You Tube,* se difunde con detalle información relacionada con el mismo, lo que contribuye a la transparencia y a que la sociedad conozca y valore la **relevante** labor judicial del Poder Judicial.

3.3.Protección de datos en las sentencias

Según nuestra CE, las sentencias serán siempre motivadas y se pronunciarán en audiencia pública (art. 120. 3 CE). En el ámbito penal, según el art. **266** de la LOPJ, las sentencias, extendidas y firmadas judicialmente, serán depositadas en la Oficina Judicial y se permitirá a cualquier interesado el acceso al texto de las mismas. Conectando lo anterior con el derecho a

la protección de datos, según el art. **235 bis de la LOPJ**, sin perjuicio de lo establecido en el párrafo 1 del art. 236 *quinquies* y de las restricciones que, en su caso, pudieran establecerse en las leyes procesales,

> *el **acceso al texto íntegro** de las sentencias, o a determinados extremos de las mismas, o a otras resoluciones dictadas en el seno del proceso, **solo** podrá llevarse a cabo **previa disociación de los datos** de carácter personal que los mismos contuvieran y con pleno **respeto** al derecho a la intimidad, a los derechos de las personas que requieran un especial deber de tutela o garantía del anonimato a las víctimas o perjudicados, cuando proceda*.

Dicho art. 236 *quinquies*, párrafo primero, LOPJ, permite al poder judicial y a los letrados de la Administración de Justicia adoptar las medidas necesarias para la supresión de datos de los documentos a los que las partes pueden acceder durante la tramitación del proceso siempre que no sean necesarios para garantizar su derecho a la tutela judicial efectiva.

Por su parte, según art. **266 LOPJ**

> *el acceso al texto de las sentencias, o a determinados extremos de las mismas, podrá quedar **restringido** cuando el mismo pudiera afectar al derecho a la intimidad, a los derechos de las personas que requieran un especial deber de tutela o garantía del anonimato de las víctimas o perjudicados, cuando proceda, así como con carácter general, para evitar que las sentencias sean usadas con fines contrarios a las leyes*.

Según el Protocolo, las **Oficinas de Comunicación** están *legitimadas para acceder al texto íntegro de las resoluciones judiciales relevantes informativamente*, en cuyo texto *se preservarán los elementos informativamente relevantes* para garantizar el derecho a la información veraz sobre hechos de trascendencia pública. Además, según el Acuerdo de 6 de abril de 2017 de la Comisión Permanente del CGPJ, también lo están para acceder a aquellas sentencias o resoluciones que resulten relevantes para el desarrollo de las actividades informativas y de relación con los medios de comunicación, al tener la condición de **interesado** a efectos del art. 235 y 266 LOPJ. Ahora bien, tienen que **respetar el criterio del órgano judicial** al aplicar lo previsto en los citados artículos citados y *velarán por su cumplimiento en la transmisión del texto de la resolución judicial a los medios de comunicación social*. Finalmente, indica que en los envíos a los medios se les **advertirá** de su responsabilidad en la difusión de datos personales contenidos en la resolución judicial, *de acuerdo al criterio establecido por los órganos técnicos afectados y el Delegado de Protección de Datos del CGPJ*.

En concreto, dicha advertencia expresará que la comunicación de la Oficina de Comunicación no significa la publicación oficial de un documento público y que la comunicación de los datos personales contenidos en la resolución judicial adjunta, sin previa disociación, se realiza en cumplimiento de su función institucional a los exclusivos efectos de su eventual tratamiento con fines periodísticos en los términos previstos por el art, 85 RGPD. Finalmente, que en todo caso será de aplicación la normativa de protección de datos al tratamiento que los destinatarios de esta información lleven a cabo de los datos que contenga la citada resolución judicial adjunta, que no podrán ser cedidos ni comunicados con fines contrarios a las leyes.

Finalmente, conviene reiterar que todas las medidas propuestas en el Protocolo de Comunicación de la Justicia, tanto en fase de instrucción penal, como de juicio oral y de publicación de las resoluciones judiciales tienen el objetivo de que la información judicial llegue a la sociedad de forma veraz, clara, eficaz y objetiva y con respeto a los derechos y libertades de los implicados, por lo que aunque no son obligatorias, sería conveniente que tales recomendaciones y medidas fueran seguidas por las Oficinas de Comunicación y por los medios de comunicación. Igualmente, es conveniente que se sigan actualizando en la sociedad digital, globalizada y cambiante a la que pertenecemos, sobre todo una vez que se presente y publique la *guía de recomendaciones en la aplicación de la normativa sobre protección de datos personales dirigida a los integrantes de la Carrera Judicial*, a la que se hace referencia expresa en el citado Informe-Propuesta del Gabinete Técnico del CGPJ en el caso de filtración de datos personales de la víctima en la sentencia de la Audiencia Provincial de Navarra nº 38/2018, en la que los órganos técnicos del CGPJ están actualmente trabajando.

Conclusiones

La protección de los datos personales no es una opción, sino un objetivo común compartido. En la Administración de Justicia, jueces y tribunales tratan, en el ejercicio de su potestad jurisdiccional y dentro de su competencia, numerosos datos personales (financieros, bancarios, familiares) de los intervinientes en los procesos judiciales. Surge la obligación de asegurar a esos sujetos (testigos, partes procesales, víctimas) la protección de su información personal, especialmente de las categorías sensibles de datos (salud, religiosos), toda vez que las consecuencias del tratamiento de datos ilícito, al margen de la normativa y de la ética son perjudiciales y de difícil reparación, la vulneración del derecho fundamental a la protección de datos personales y, por ende, el incumplimiento de la normativa sobre protección de datos.

La normativa general europea sobre protección de datos abarca el RGPD, en vigor desde mayo de 2018, adaptado al ordenamiento español por la LOPDGDD 3/2018, aunque dicho Reglamento sigue teniendo aplicación directa, y la Directiva 2016/680 (DPDP, en adelante) que tiene que ser traspuesta al Derecho nacional. Para garantizar la protección de datos en la Administración de Justicia española, ésta ha sido dotada por la reforma de 2015 de la LOPJ de un régimen jurídico particular que consiste en aplicar a la citada normativa general (RGPD y LOPDGDD) las especialidades previstas en la LOPJ (art. 236 *bis* a art. 236 *decies)* en todos los órdenes jurisdiccionales, excepto en el penal, donde se aplica la DPDP 2016/680, igualmente con las especialidades de la LOPJ. Sin embargo, hasta que dicha Directiva sea transpuesta, siguen siendo de aplicación los arts. 22 y sus disposiciones de desarrollo de la antigua LOPD 1999.

Las particularidades básicas de dicho régimen específico consisten en que se distinguen dos tipos de ficheros de datos tratados por los órganos judiciales u Oficina Judicial en relación con los incorporados a los procesos de que conozcan: jurisdiccionales y no jurisdiccionales. Respecto al tratamiento de los primeros, no se aplica el consentimiento del interesado como base de legitimación, sino que se acude al resto de las bases previstas en el art. 6 RGPD, normalmente, el ejercicio de la potestad jurisdiccional (misión en interés público u obligación legal), sin perjuicio de lo dispuesto en las normas procesales para la validez de la prueba.

El responsable del tratamiento en relación con los ficheros jurisdiccionales es el órgano judicial, u Oficina Judicial, ante el que se tramite el procedimiento y, en concreto, el juez o letrado de la Administración de Justicia de cada juzgado, según sus funciones y competencias, pero las Administraciones Públicas competentes en materia de dotación de medios materiales son también corresponsables, en su respectivo territorio.

El CGPJ es la autoridad de control del cumplimiento de la protección de datos en relación con los ficheros jurisdiccionales, ejerciendo las competencias que la AEPD (o autoridades autonómicas correspondientes) posee sobre los ficheros no jurisdiccionales. Por ello, no es crear otro organismo específico de control diferente al CGPJ, sino que, en su caso, se podría plantear reforzar su independencia en el cumplimiento de la función de autoridad de control, conforme el RGPD.

Consecuencia de las reformas legales y de las tendencias europeas, sería conveniente elaborar una regulación sistemática, completa, desarrollada, de la protección de datos en la Administración de Justicia, pues el actual régimen formado por tan solo nueve artículos con remisiones a otras normas ha devenido insuficiente. Hemos de ser positivos. Se va por buen camino y se ha avanzado considerablemente en cuanto a la protección de datos en este ámbito; pero también realistas, siempre se puede y debe mejorar. Es importante aprender de los errores pasados para proyectar que no se vuelvan a repetir. Seguir trabajando en la consecución del objetivo común, un mayor nivel de protección de datos; en que se siga impartiendo formación y actualización periódica sobre esta materia al personal integrante y al servicio la Administración de Justicia; y en la colaboración y coordinación de todas las instituciones en la protección de los datos de los intervinientes en los procesos judiciales. Todo ello favorecerá la tutela y la responsabilidad proactiva en el cumplimiento de este derecho fundamental. Igualmente, contribuirá a fomentar la cultura social de protección de datos.

Los recientes casos de filtraciones de datos inciden directamente en la percepción de la ciudadanía de la justicia como *mejorable* y cuestionan el tratamiento de los datos en la Administración de Justicia. Los órganos judiciales son fuentes de interés periodístico. Los medios de comunicación tienen un papel esencial en el ejercicio del derecho a la información del que son titulares los ciudadanos, como también lo son de la protección de sus datos personales. Las Oficinas de Comunicación *son la piedra angular* de la política de comunicación del CGPJ. Sin ellas no es posible trasladar la actividad judicial a la sociedad ni cumplir con el deber de transparencia. Una política de transparencia, mediante la comunicación de información puntual, veraz, objetiva y responsable, con respeto de los derechos y libertades, es el mejor modo de impedir interpretaciones indeseadas o erróneas por parte de los implicados en el proceso o terceros, especialmente en la fase de instrucción penal.

La elaboración por parte de la Oficina de Comunicación del CGPJ de Protocolos de Comunicación de la Justicia, el actual de 2018, con recomendaciones concretas para que la información judicial llegue a la sociedad de forma veraz, clara, eficaz y objetiva y con respeto a los derechos y libertades de los implicados, merece una valoración muy positiva. Es conveniente que este Protocolo, pese a no ser de obligado cumplimiento, sea tenido en cuenta por parte de las Oficinas de Comunicación y los medios de comunicación, en aras de que los derechos y principios implicados (información, publicidad de actuaciones, tutela judicial efectiva, intimidad, honor, protección datos personales) convivan de forma pacífica. Igualmente, que sea actualizado cuando se presente y publique la *guía de recomendaciones en la aplicación de la normativa sobre protección de datos personales dirigida a los integrantes de la Carrera Judicial*, en la que los órganos técnicos del CGPJ están actualmente trabajando.

[1] Este es el sentido del art. 230 de la LOPJ y de la Instrucción del CGPJ, de noviembre de 2018, que expresa que jueces y magistrados deben utilizar medios informáticos, establece los requisitos que han de reunir para que se exija su obligatoriedad y las condiciones que deben satisfacerse en relación con la formación sobre su uso y las políticas de prevención de salud profesional. No obstante, según el Acuerdo de 22 de noviembre de 2018, de la Comisión Permanente del CGPJ, por el que se aprueba la Instrucción 1/2018, mientras dichos programas y herramientas no sean obligatorios se les deberá garantizar expedientes en papel, sea porque su tramitación se lleva a cabo de dicha forma, sea porque se establezca un expediente paralelo o duplicado en papel. De ahí que, actualmente, en la Oficina Judicial encontremos expedientes en papel, electrónicos y mixtos, considerándose que estos últimos pueden tener más inconvenientes que ventajas.

[2] A efectos del RGPD, *tratamiento* es toda operación o conjunto de ellas sobre datos personales, por procedimientos automatizados o no, como la recogida, registro, organización, conservación, modificación, consulta, utilización, difusión o cualquier otra forma de habilitación, cotejo o interconexión, limitación, supresión o destrucción (art. 4. 2 RGPD).

[3] Más información sobre la protección de datos en América Latina en LÓPEZ MEDINA C. "Protección de datos en América Latina y las tendencias actuales", Blog Jurídico *Bajo la Toga,* febrero 2019, disponible en https://bajolatoga.com/2019/02/15/proteccion-de-datos-personales-en-america-latina-y-las-tendencias-actuales-por-carolina-lopez-medina/
(consultado el 13 de marzo de 2019)

[4] Según el TC, el derecho a la libertad de información es *la difusión de aquellos hechos que merecen ser considerados noticiables*, a diferencia de la libertad de expresión, *cuyo objeto son los pensamientos, ideas y opiniones (concepto amplio que incluye las apreciaciones y los juicios de valor* (STC 79/2014, de 28 de mayo, F.J. 4).

[5] Véase la sinopsis del artículo 20 CE, realizada por ELVIRA PERALES, A. en diciembre de 2003, actualizada en enero de 2011, por GONZÁLEZ ESCUDERO A.
Recuperado de:
http://www.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=20&tipo=2.
(consultado el 13 de marzo de 2019)

[6] "Facebook eleva a 87 millones los usuarios afectados por el escándalo de Cambridge Analytica". Recuperado de: http://www.europapress.es/internacional/noticia-facebook-eleva-87-millones-usuarios-afectados-escandalo-cambridge-analytica-20180404212958.html, 2018.
(consultado el 13 de marzo de 2019)

[7] "*Se filtran los resultados del MIR 2018 y del EIR antes de que los publique el Ministerio de Sanidad*".
Recuperado de:
http://www.elmundo.es/espana/2018/03/05/5a9d92d9e2704e157d8b45d4.html, 2018
(consultado el 13 de marzo de 2019)

[8] Recuperado de:
https://www.elmundo.es/economia/empresas/2019/01/21/5c45e159fc6c8305148b4693.html
(consultado el 13 de marzo de 2019)

[9] Recuperado de: https://www.svpe-ples.org/index.php/noticias/145-abren-expediente-a-la-policia-de-getxo-por-revelar-las-multas-que-pone-cada-agente, 2019.
(consultado el 13 de marzo de 2019)

[10] Recuperado de:
https://elpais.com/politica/2019/03/08/actualidad/1552045894_161671.html,2019.
(consultado el 13 de marzo de 2019)

[11] DELGADO MARTÍN, J. (2019). "Reflexiones sobre la protección de datos personales en la Administración de Justicia", *Diario La Ley,* nº 9363, Sección Tribuna, 21 de febrero, Wolters Kluwer, p.4.

[12] Ibidem, p.13ss.

[13] Disponible en la web del CGPJ:http://www.poderjudicial.es/cgpj/es/Poder-Judicial/En-Portada/El-CGPJ-concluye-que-la-filtracion-de-datos-personales-de-la-victima-en-la-sentencia-de-la-Audiencia-de-Navarra-38-2018-se-debio-a-multiples-causas-que-propiciaron-un-fallo-de--caracter-sistemico- (consultado el 13 de marzo de 2019)

[14] Recuperado de:
https://retina.elpais.com/retina/2017/08/11/tendencias/1502446063_042539.html, 2017
(consultado el 13 de marzo de 2019)

[15] Recuperado de
http://www.elmundo.es/comunidad-valenciana/2018/04/26/5ae1a3c7ca4741995d8b4678.html. (consultado el 13 de marzo de 2019)

[16] El Protocolo de Comunicación de Justicia 2015 adecuó el Protocolo anterior de 2004 a la LO 4/2013, de reforma del CGPJ. Se trata de responder a los cambios en el sector de la comunicación y a la relevancia social e informativa que ha adquirido la actividad de los juzgados y tribunales.

[17] BERBELL C. (2019). Ponencia sobre Transparencia en la Justicia española, en el marco de Pasantía de Magistratura Contemporánea: La Justicia en el siglo XXI. Sede del Servicio de Formación Continua del CGPJ, 18 de febrero de 2019.

[18] Ibidem.